

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the Getting Started Guide, which are available from Trend Micro's Web site at:

www.trendmicro.com/download

NOTE: A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be reviewed on an annual basis at Trend Micro's then-current Maintenance fees.

Trend Micro, the Trend Micro t-ball logo, and PC-cillin are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Copyright© 2005 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Document Part No. PCEM32404/50824

Release Date: October 2005

The Getting Started Guide for Trend Micro™ PC-cillin™ Internet Security is intended to provide an overview of the product and deployment instructions for your test or production environment. Read it prior to deploying PC-cillin Internet Security.

For technical support, please refer to *Technical Support* for contact details. For detailed configuration instructions and protection strategies, refer to the *PC-cillin Internet Security Online Help* and *Context sensitive help*, which is accessible from the PC-cillin Internet Security main console.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

www.trendmicro.com/download/documentation/rating.asp

Contents

Preface

Documentation	2
About this Getting Started Guide	2
Audience	3
Document Conventions	3

Chapter 1: Introduction

What's New	6
Protection Features	15
Preconfigured Protection	16
Main Console	17
Action Buttons and System Tray Icons	18

Chapter 2: Installation

Hardware and Software Requirements	20
Before Installation	22
Upgrade from a Previous Release	23
Install PC-cillin Internet Security 2006	26
After Installation	33
Uninstall PC-cillin Internet Security	34

Chapter 3: Get Started

Register or Activate the Product	38
Use the Registration/Activation Page	39
Use the Main Console	40
Verify a Successful Installation	42
Access the Main Console	43
Check Current Settings	45
Update Components	46
Automatically Update Components	46
Manually Update Components	47
Password-protect the Program	50
Obtain More Help	51

Chapter 4: Problem Solving and FAQ

Installation	54
Registration/Activation	56
Main Console Access Issues	57
Component Update Issues	58
Frequently Asked Questions	59
General	59
Serial Number, Installation, and Registration	59

Chapter 5: Technical Support

Contact Technical Support	66
Send Infected File Samples	67
Report Spam, Fraudulent, and Incorrectly Tagged Messages	67
TrendLabs	67
Other Useful Resources	68

Index

Preface

Welcome to the Trend Micro™ PC-cillin™ Internet Security *Getting Started Guide*. This book contains basic information about the tasks you need to install the software. It is intended for first time and advanced users who want to learn about, install, and get started with PC-cillin Internet Security.

This Preface discusses the following topics:

- *Documentation* on page 2
- *About this Getting Started Guide* on page 2
- *Audience* on page 3
- *Document Conventions* on page 3

Documentation

The PC-cillin Internet Security documentation consists of the following:

- *Online Help*—compiled HTML-based documentation that is accessible from the product's main console

It contains explanations about the product's components and features, which includes procedures needed to perform specific tasks from the main console, problem solving instructions, examples, and demonstrations.

- *Getting Started Tutorial*—HTML-based documentation that provides guidance on how to maximize the product's features
- *Getting Started Guide (GSG)*—PDF documentation that is accessible from the Trend Micro PC-cillin Internet Security CD or can be downloaded from the Trend Micro Update Center (<http://www.trendmicro.com/download/>)

This GSG contains instructions on how to install the product, as well as testing, problem solving, and post-installation instructions. See [About this Getting Started Guide](#) for chapters available in this book.

Tip: Click the PC-cillin Internet Security link from the Update Center (<http://www.trendmicro.com/download>) for updates to the PC-cillin Internet Security documentation and program files.

About this Getting Started Guide

This *Getting Started Guide* discusses the following topics:

- *Introduction*—an overview of the product and its components
- *Installation*—procedures to install, upgrade, renew, or remove the product
- *Get Started*—post-installation configurations to help you get started
- *Problem Solving and FAQ*—troubleshooting tips for issues encountered when installing the product or performing post-installation tasks
- *Technical Support*—guidelines for obtaining more information

Audience

The PC-cillin Internet Security documentation assumes a basic knowledge of computers, including:

- Antivirus, antispyware, and content security protection
- General network concepts, such as IP addressing, the Internet, and firewalls

Document Conventions

To help you locate and interpret information easily, the PC-cillin Internet Security documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and service or process names
<i>Italics</i>	References to other documentation
Monospace	Examples, sample command lines, program code, Web URLs, file names, folder names, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

TABLE 1. Conventions used in the PC-cillin Internet Security documentation

Introduction

1

This chapter introduces PC-cillin Internet Security and provides an overview of its features.

The topics discussed in this chapter include:

- *What's New* on page 6
- *Protection Features* on page 15
- *Preconfigured Protection* on page 16
- *Main Console* on page 17

After learning the PC-cillin Internet Security concepts in this chapter, proceed to the following sections:

- *Hardware and Software Requirements* for system requirements
- *Before Installation* for pre-installation tasks and other considerations
- *Upgrade from a Previous Release* if your computer has PC-cillin Internet Security installed
- *Install PC-cillin Internet Security 2006* for installation instructions
- *Get Started* for post-installation instructions

What's New

Trend Micro PC-cillin Internet Security 2006 provides the following features:

- *Full or Minimum Installation*
- *Antiphishing*
- *Complete Scan*
- *Antifraud Wizard*
- *Antifraud Toolbar in Internet Explorer*
- *Complete Antispyware Features*
- *Blocking Extra Hosts File Entries and Spoofed Domain Names*
- *Scheduled Vulnerability Check*
- *Popup Manager*
- *Revert Feature*
- *Enhanced Usability*

Full or Minimum Installation

The **Full** installation allows you to install all features of PC-cillin Internet Security. Alternatively, the **Minimum** installation will install all features except the following:

- **Real-time Network Virus Protection**—runs in the background to protect your computer from malicious network packets
- **Personal Firewall**—helps protect you against hackers damaging files, stealing personal information, or creating mischief
- **Wi-Fi Intrusion Detection**—monitors a wireless Ethernet (Wi-Fi) network and warns of unwanted intrusions

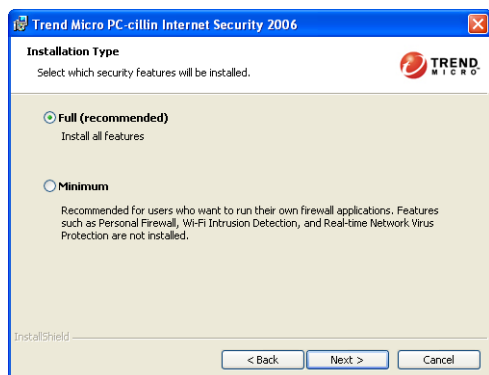


FIGURE 1-1. Installation Type screen

If you wish to keep your existing firewall program, select the **Minimum** installation.

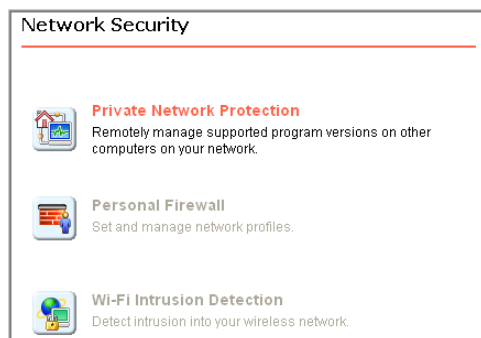


FIGURE 1-2. PC-cillin Internet Security, installed with the **Minimum** option

Antiphishing

Phishing is a rapidly growing form of fraud that seeks to fool Web users into divulging private information by mimicking a legitimate Web site. To learn more about phishing, please refer to the PC-cillin Internet Security *Online Help* > *Learn About...* section. Alternatively, visit the FAQ topic on [page 61](#).

PC-cillin Internet Security 2006 uses the following features to help prevent phishing attacks:

- **Fraud Filter**—provides protection against fraudulent messages

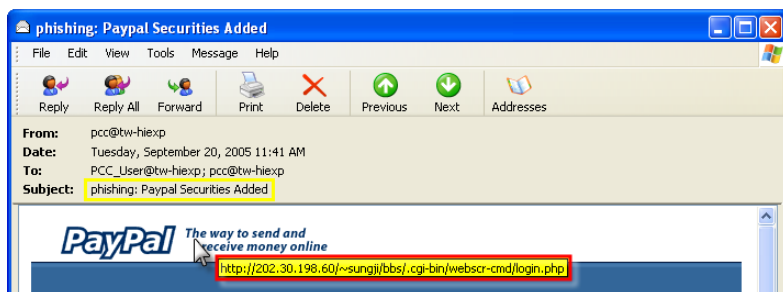


FIGURE 1-3. The Fraud Filter identifies phishing messages and adds the subject prefix phishing:

Tip: Move your mouse over the links to display the actual address. If the link displayed on a message differs from the link displayed on the status bar, the email message is likely spoofed and part of a fraudulent attack.

- **Web Site Filter**—provides protection against fraudulent Web sites

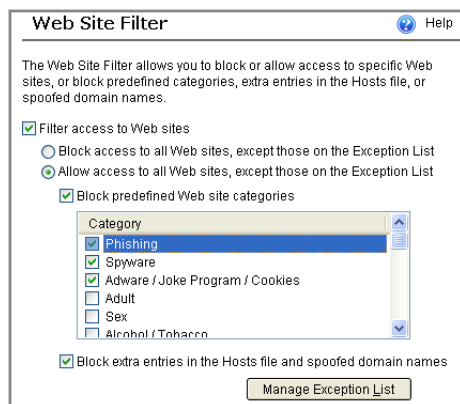


FIGURE 1-4. The Web Site Filter lets you make certain Web sites *off limits*, block extra entries in the Hosts file, and block spoofed domain names

Complete Scan

Complete Scan provides you with the option to scan for viruses, spyware, and other threats on demand from the **Overview** screen of the PC-cillin Internet Security main console.

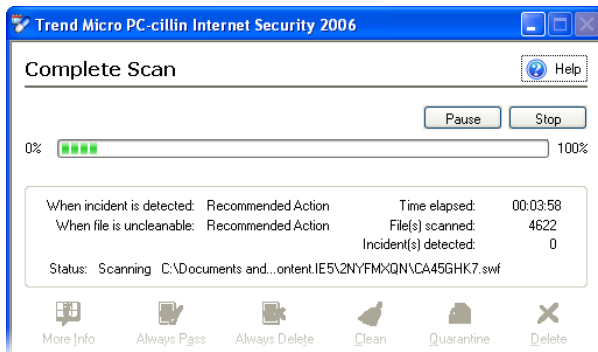


FIGURE 1-5. Complete Scan in progress

Tip: Alternatively, run Complete Scan by clicking **Scan Now** from the program's system tray menu.

Antifraud Wizard

The Antifraud Wizard provides a step by step guide to help you configure settings for protection against phishing, pharming, and other fraudulent attacks.

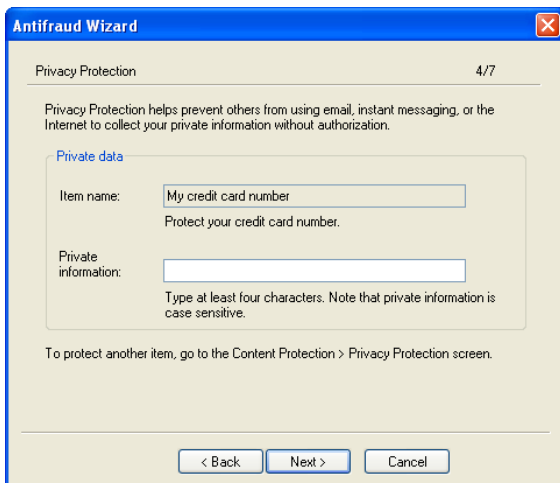


FIGURE 1-6. Antifraud Wizard

Antifraud Toolbar in Internet Explorer

The Antifraud Toolbar helps keep you safe from fraudulent or potentially offensive Web sites. It is turned off by default.

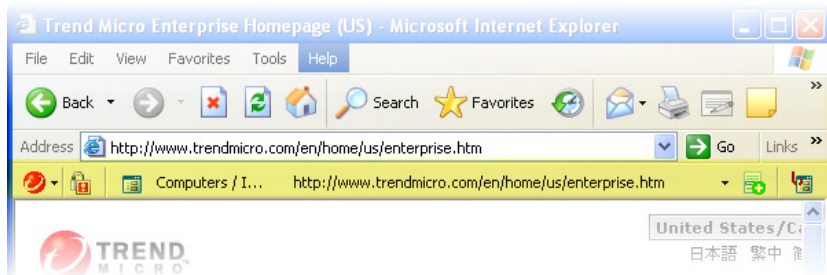


FIGURE 1-7. The Antifraud Toolbar in Internet Explorer

Complete Antispyware Features

PC-cillin Internet Security provides you with complete spyware protection including:

- Real-time Spyware Protection that guards you against spyware, adware, and other grayware
- Manual Spyware Scan to detect and eliminate grayware between scheduled spyware scans
- Scheduled Spyware Scan to detect and eliminate grayware on an automatic schedule you set



FIGURE 1-8. The Antispyware screen

Blocking Extra Hosts File Entries and Spoofed Domain Names

The Web Site Filter incorporates extra Hosts file entry and spoofed domain name blocking. This feature filters and blocks extra entries in the Hosts file or

spoofed domain names that aim to trick you into visiting illegal or spoofed Web sites.

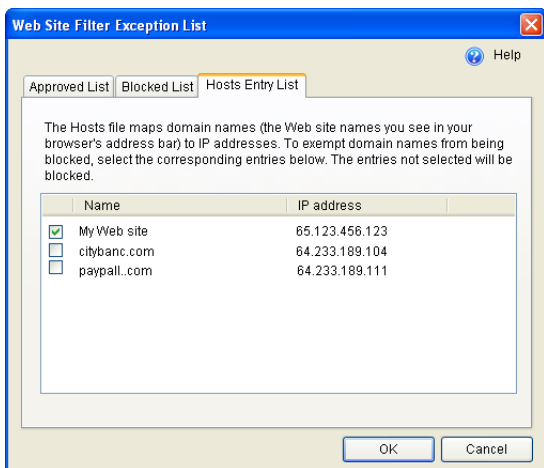


FIGURE 1-9. Web Site Filter > Hosts File Filtering

Scheduled Vulnerability Check

In addition to manual Vulnerability Check, PC-cillin Internet Security now lets you schedule daily, weekly, or monthly Vulnerability Check.

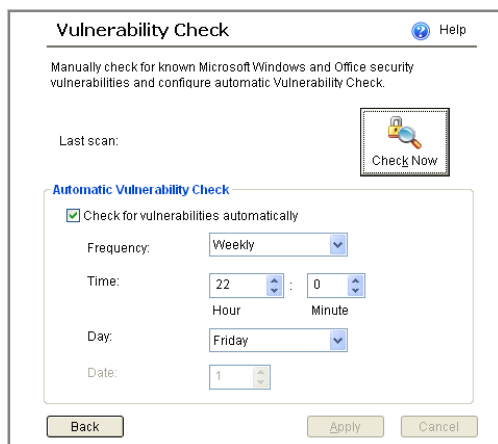


FIGURE 1-10. The Vulnerability Check screen

Popup Manager

The Popup Manager lets you customize the available popup messages. Popup messages are a good way to be informed of specific program actions and events.

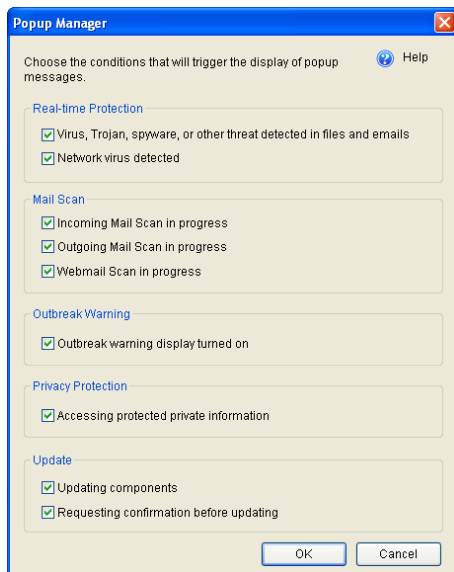


FIGURE 1-11. Popup Manager

Revert Feature

The Update feature provides a **Revert** option, also known as rollback, that automatically attempts to stabilize the computer's behavior whenever a program, hardware, or network error causes the computer to be unstable.

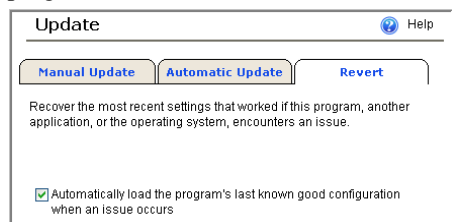


FIGURE 1-12. The Revert screen

Enhanced Usability

The new menu categorization (see Figure [1-14](#)), along with mouseover help messages and the Getting Started tutorial, help users understand and configure the program's features.

Protection Features

Trend Micro designed PC-cillin Internet Security to protect your computer from both external and internal threats. This table illustrates how PC-cillin Internet Security helps protect you and your assets against known threats:

THREAT	PROTECTION
Viruses, Trojans, worms, and other malicious programs	Virus Scan
Spyware and additional Internet threats that could alter your Hosts file or Registry	Spyware Scan
Viruses, Trojans, worms, and other malicious programs that could be contained in messages and attachments	Mail Scan
Spam or unsolicited commercial messages	Spam Filter
Phishing messages	Fraud Filter
Virus outbreaks	Virus Scan, Spyware Scan, Real-time Network Virus Protection
Hackers	Personal Firewall
Intrusion into wireless networks	Wi-Fi Intrusion Detection
Unauthorized collection of private information via Web, email, or instant messages	Privacy Protection
Known Microsoft™ Windows™ and Office security vulnerabilities	Vulnerability Check

TABLE 1-1. Protection features of PC-cillin Internet Security

Preconfigured Protection

As installed, without changing any settings, PC-cillin Internet Security does the following:












- Checks for and downloads component updates every three hours
- Checks for viruses every time you open, copy, move, or save a file
- Protects against downloading infected files
- Blocks spyware and other grayware
- Protects your computer against hackers and network viruses

Note: If you selected the Minimum installation type (see [page 7](#)), the Personal Firewall and Real-time Network Virus Protection features are not available.

- Scans incoming or outgoing email messages and attachments as they are being downloaded from the POP3 server or sent via an SMTP server

If applicable to your computing environment, Trend Micro recommends enabling Spam and Fraud Filters, Web Site Filter, and Privacy Protection.

Tip: The Protection Summary screen of the main console lists the features currently turned on. To access the Protection Summary screen, click the **Configure** button adjacent to **Protection** on the **Overview > Summary** screen.

Protection Summary Help	
 Real-time Virus Protection	Turned on
 Real-time Network Virus Protection	Turned on
 Incoming Mail Scan	Turned on
 Outgoing Mail Scan	Turned on
 Webmail Scan (*)	Turned off
 Real-time Spyware Scan (*)	Turned on
 Spam and Fraud Filters (*)	Turned off
 Web Site Filter (*)	Turned off
 Privacy Protection (*)	Turned off
 Personal Firewall	Turned on
 Wi-Fi Intrusion Detection (*)	Turned off

* - Optional settings

FIGURE 1-13. The Protection Summary screen


Main Console

From the PC-cillin Internet Security main console, you have access to the program's settings and summary information. Each button on the left side of the console lets you view or manage the settings for a particular security or antivirus area.



FIGURE 1-14. The main console

The **header menu** is on the topmost part of the main console. It provides the same options as the main menu, in drop down format. The header menu is turned off by default.

Tip: To display the header menu, click the program icon () on the left-hand top-most corner of the main console, and select **View header menu**.

The **main menu** is on the left-hand area of the main console. It provides access to all features and options.

The **working area** is the place where you configure the program settings and open the subwindows for additional product configuration.

The **footer menu** is found at the bottom part of the main console. It provides links to the **Contents and Index**, **Virus Information**, **Technical Support**, **Customer Care Center**, and **About**.

Action Buttons and System Tray Icons

Use the table below to identify the meanings of common program buttons and system tray icons:












BUTTON / ICON	DESCRIPTION
	Runs a Complete Scan, Manual Virus Scan, or Manual Spyware Scan.
	Runs a manual component update.
	Returns to the last visited screen. Note: Clicking the Back button available on screens with tabs will open the landing page for the screen. For example, clicking Back on the Mail Scan > Webmail tab will open the Antivirus screen.
	Opens the feature's working area for configuration.
	Closes a subwindow and saves any configuration changes that were made.
	Saves the configuration changes made.
	Closes a subwindow and discards the configuration changes made.
	Signifies that all incoming and outgoing Internet traffic has been stopped.
	Signifies that PC-cillin Internet Security is connecting to the Trend Micro server to download the latest updates.
	Signifies that Real-time Scan is turned on.
	Signifies that Real-time Scan is turned off.

TABLE 1-2. Common program buttons and icons

Installation

This chapter explains how to plan and prepare for a PC-cillin Internet Security installation.

The topics discussed in this chapter include:

- *Hardware and Software Requirements* on page 20
- *Before Installation* on page 22
- *Install PC-cillin Internet Security 2006* on page 26
- *After Installation* on page 33
- *Uninstall PC-cillin Internet Security* on page 34

Hardware and Software Requirements

Table 2-1 lists the hardware and software requirements for PC-cillin Internet Security.

HARDWARE/SOFTWARE REQUIREMENTS	REQUIREMENTS
CPU	<ul style="list-style-type: none"> Intel Pentium™ 233MHz or equivalent processor for Windows 98, 98 Second Edition (SE), or Millennium Edition (Me) Intel Pentium 300MHz or equivalent processor for Windows 2000 or XP
Memory	128MB RAM
Hard disk space	100MB of available hard disk space for installation Note: In addition, this version supports Intel Hyper-Threading and Dual-Core Processors, and RAID 0 (Striping) or RAID 1 (Mirroring or Duplexing).
Operating system	<ul style="list-style-type: none"> Windows 98, 98SE, or Me Windows 2000 Professional with SP4 Windows XP Home or Professional with Service Pack 1 (SP1) or 2 (SP2) Windows XP Media Center Edition 2004 or 2005 Windows XP Tablet PC Edition 2004 or 2005
Mail User Agent (MUA)—Email Software for Incoming/Outgoing Mail Scan	<ul style="list-style-type: none"> Becky! Internet Mail 2.0 Eudora 6.2 Microsoft Outlook Express 6.0 Microsoft Outlook 2000, 2002, or 2003 Mozilla Thunderbird 1.0 Netscape 7.2
Web based mail services for Webmail Scan	<ul style="list-style-type: none"> AOL Mail services Microsoft Hotmail Yahoo! Mail

TABLE 2-1. PC-cillin Internet Security system requirements

HARDWARE/SOFTWARE REQUIREMENTS	REQUIREMENTS
Web browser	<ul style="list-style-type: none"> • AOL Browser 9.0 Security Edition • Microsoft Internet Explorer 5.5 with SP2 for computers running Windows 98, 98SE, or Me • Microsoft Internet Explorer 6.0 with SP2 for computers running Windows XP SP2 • Microsoft Internet Explorer 6.0 SP1 for computers running Windows 98, 98SE, Me, 2K, or XP with SP1 • Mozilla Firefox 1.0 • Netscape™ 7.2
Instant messaging clients for Privacy Protection	<ul style="list-style-type: none"> • AOL Instant Messenger 5.9 • ICQ 5 or ICQ Lite • MSN Messenger 7.0 • Windows Messenger 4.7 or 5.1
General	<ul style="list-style-type: none"> • A monitor with a resolution of 800 x 600 pixels or higher, and High Color (65536 colors) or greater color depth • Adobe™ Acrobat™ is required to view the Getting Started Guide. Download the free Acrobat Reader™ software at http://www.adobe.com • An Internet connection is necessary to register online, download updates, obtain virus information, browse pages on the Trend Micro Web site, or send email messages. <p>Note: If you have a dial-up or other connection to the Internet that charges fees per connection and/or per amount of time connected or data downloaded, make sure your router or connection software does not automatically start a connection for the Automatic Update feature. This could result in an extra connection fee. Modify the router settings as required, or turn off Automatic Update. Please refer to your router's documentation for instructions.</p>

TABLE 2-1. PC-cillin Internet Security system requirements

Before Installation

Several pre-installation tasks can help to make the installation process easier. Complete the following tasks before installing PC-cillin Internet Security:

- Check that the target computer (the computer upon which the program will be installed) complies with the hardware and software requirements. If the computer's specifications do not meet the requirements (see [Table 2-1](#) on [page 20](#)), Setup will not install PC-cillin Internet Security.
- If the target computer is running a previous version of the product, uninstall it before upgrading to the latest release (see [page 23](#) for details about upgrading).
- If a firewall program such as Windows firewall is running on the target computer, decide whether or not to keep the program running.

To avoid incompatibilities with other firewall programs, Setup lets you choose between **Full** or **Minimum** installation type (see [page 31](#)).

Tip: Trend Micro recommends running the PC-cillin Internet Security Personal Firewall.

- Log on to the target computer using an account with **Administrator** privileges.
Setup requires a user with Administrator privileges to install and register the program components.
- Uninstall other antivirus programs to prevent scanning conflicts.
- If you connect to the Internet through a proxy server, obtain the proxy server information from your system administrator or ISP.

Note: Proxy servers are frequently used in businesses or schools, as well as by some Internet Service Providers (ISPs).

PC-cillin Internet Security uses the proxy server settings specified to connect to the Internet during product registration, Personal Firewall detection, and component update.

- Close all open programs.
- Prepare the standard, evaluation, or OEM version serial number (see [page 23](#)).

If PC-cillin Internet Security 2005 or PC-cillin Internet Security 2004 is installed, keep a copy of the serial number used. You can use the serial number to install PC-cillin Internet Security 2006.

After completing the pre-installation tasks, proceed by installing (see [page 26](#)) and registering or activating the product (see [page 38](#)).

Upgrade from a Previous Release

Upgrade to the latest version if you are using one of the following versions:

- An evaluation, original equipment manufacturer (OEM), or beta version of PC-cillin Internet Security 2006
- PC-cillin Internet Security 2005

Note: During an upgrade, PC-cillin Internet Security deletes all logs, quarantined files, and entries in the Approved and Blocked lists. Quarantined files may contain viruses and should not be left on your computer. If you must preserve them, restore the files to a safe, isolated location such as a specially marked floppy disk before removing the program. For instructions on how to restore quarantined files, please refer to the PC-cillin Internet Security *Online Help*.

To upgrade from a previous release:

1. Obtain and write down the serial number from one of the following:

- Trend Micro confirmation email message, which Trend Micro sends when you register a standard version or activate an evaluation or OEM version of the product

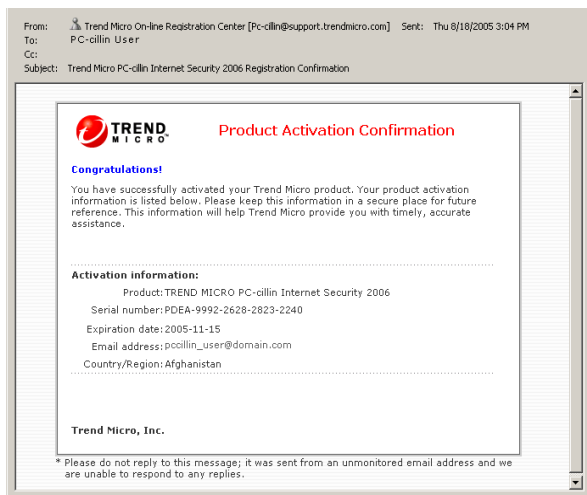



FIGURE 2-1. Sample confirmation message after activating an evaluation or OEM version

- PC-cillin Internet Security main console—applicable if you are using an evaluation, OEM, beta version, or previous product releases, such as PC-cillin Internet Security 2005
 - i. Open the PC-cillin Internet Security main console by double-clicking the Real-time Scan icon () in the system tray.
 - ii. Click **Help > About**.

The serial number appears in the License information section.

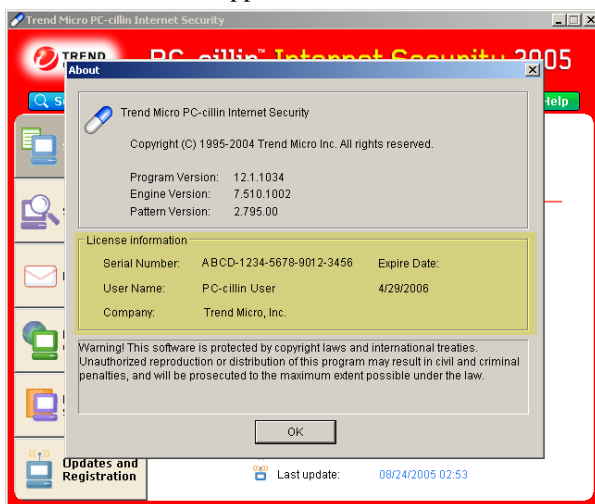


FIGURE 2-2. A sample serial number as shown in the PC-cillin Internet Security 2005 main console's About window

- Product package—does not apply if you are upgrading from an evaluation, OEM, or beta version of PC-cillin Internet Security 2006
 - i. Locate the original package.
 - ii. Open the booklet that contains the CD and manual.
The CD and serial number are located on the left page of the booklet.
The manual is on the right side.
2. Uninstall the previous release (see [page 34](#) for instructions).
 3. Follow the installation steps on [page 26](#).

Install PC-cillin Internet Security 2006

Installing Trend Micro PC-cillin Internet Security is simple and only takes a few minutes.

Tip: Complete the tasks on [page 22](#) before installing PC-cillin Internet Security 2006. If you are upgrading from a previous release, read the instructions on [page 23](#) first.

To install PC-cillin Internet Security:

1. Start the Setup program by performing one of the following steps:
 - If you are using the installation file downloaded from the Trend Micro Web site (<http://www.trendmicro.com/download>), save the installation file in a temporary location.

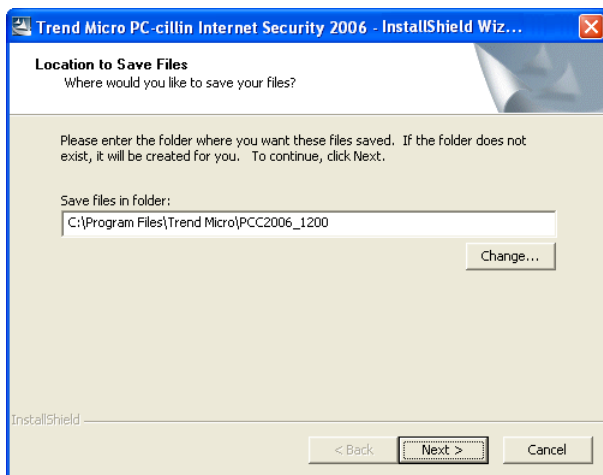


FIGURE 2-3. Starting Setup from the downloaded installation file

- If you are using the PC-cillin Internet Security CD, insert the CD into your CD-ROM drive, and perform any of the following:
 - If the menu automatically appears, click **Install Program**, and then click **Next**

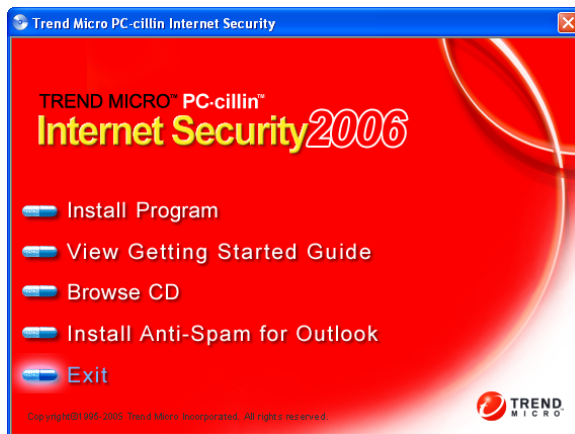


FIGURE 2-4. Launching Setup from the PC-cillin Internet Security CD main menu

- If the menu does not automatically open, from the Windows Taskbar, click **Start > Run**



Tip: Alternatively, on Windows desktop, double-click the **My Computer** icon, and then navigate to your computer's CD drive.

In the **Open** field, type `<CD drive>:\Setup\setup.exe` and click **OK**.

`<CD drive>` is the drive letter of your CD-ROM, for example E.

The Welcome screen appears. Click **Next**.

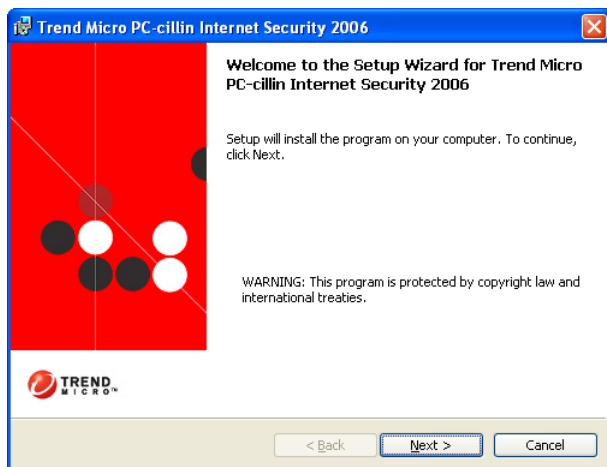


FIGURE 2-5. Welcome screen

2. Read the license agreement, and then click **I accept the terms in the license agreement** to continue installing PC-cillin Internet Security.

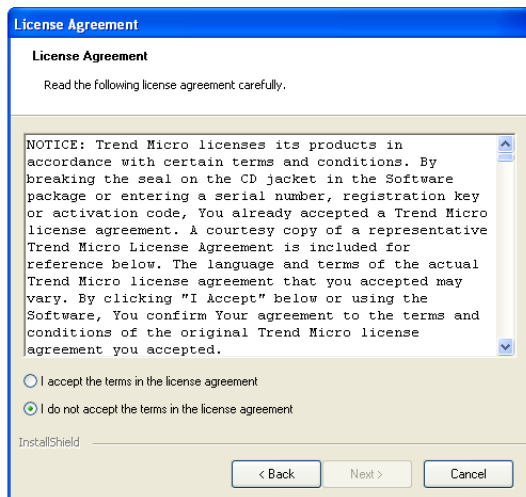


FIGURE 2-6. License Agreement screen

The installation procedure stops if you do not accept the terms.

3. Click **Next**. PC-cillin Internet Security scans your computer's memory, boot sector, and critical files before installing the program files.

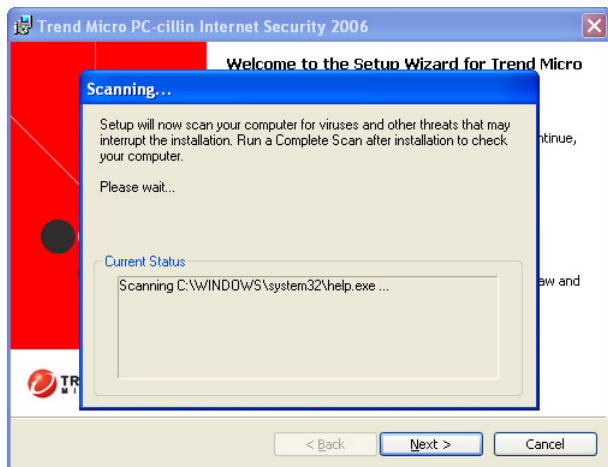


FIGURE 2-7. Scanning notice

If PC-cillin Internet Security cleans or deletes any infected files found.

4. Click **Next**. The Product Registration screen appears.

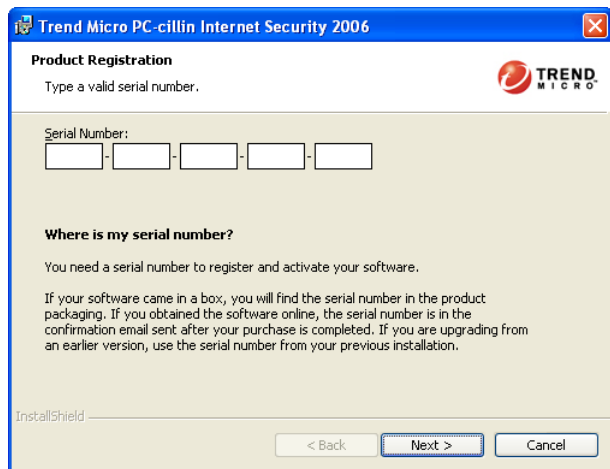


FIGURE 2-8. Product Registration screen

If you are installing an evaluation version, type the evaluation serial number. Otherwise, if you are installing the standard version, type the standard version serial number.

Note: The Setup program of PC-cillin Internet Security 2006 accepts the serial number used in PC-cillin Internet Security 2005 or PC-cillin Internet Security 2004.

5. Click **Next**. The Installation Folder screen appears. You can install PC-cillin Internet Security in the default location, or choose a different location.

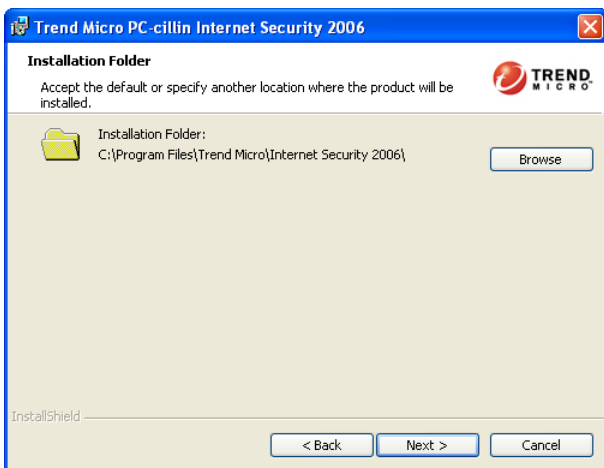


FIGURE 2-9. Installation Folder screen

To change the installation location click **Browse**, and select the location to which PC-cillin Internet Security installs.

6. Click **Next**. The Installation Type screen appears. You can install the full version of PC-cillin Internet Security, or only specific functions.

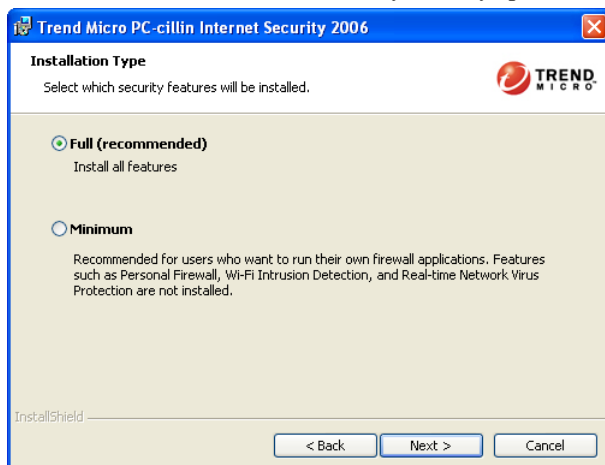


FIGURE 2-10. Installation Type screen

Selecting **Full** when your computer has other firewall programs running, such as Windows Firewall, will cause Setup to display message below. Refer to [page 22](#) for details that will help you decide which installation type is suited for your computing needs.

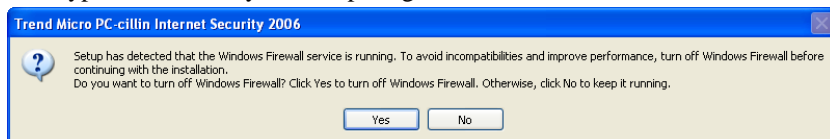


FIGURE 2-11. If you select **Full** installation but have another firewall program installed, this message appears

Selecting **Minimum**, will exclude the PC-cillin Internet Security Personal Firewall, Wi-Fi Detection, and Real-time Network Virus Protection features from installation.

Tip: Trend Micro recommends that you select **Minimum** only if you wish to keep your current firewall program(s).

7. Click **Next**. If you are satisfied with the selections you have made, click **Install** to begin installation.

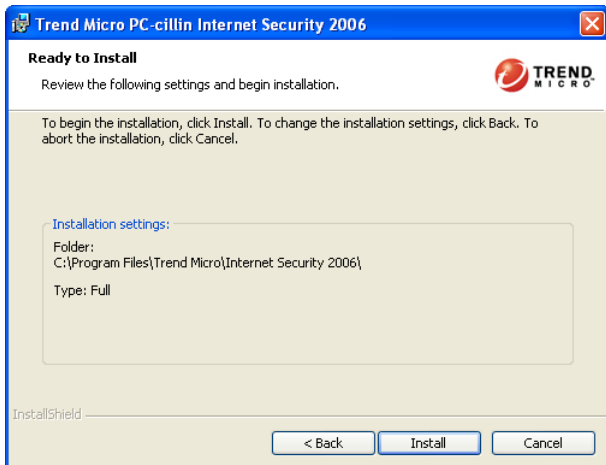


FIGURE 2-12. Ready to Install screen

Setup begins to install the program.

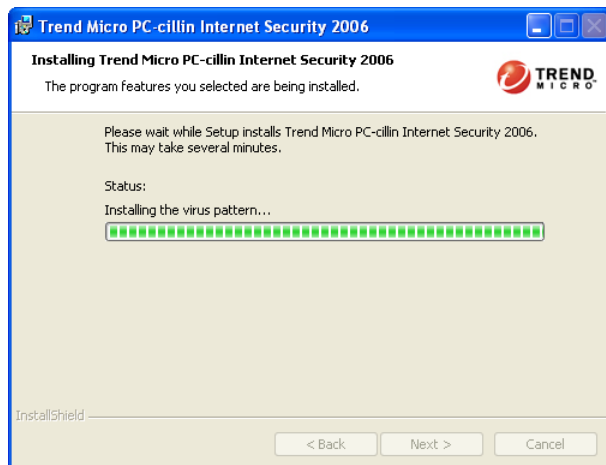


FIGURE 2-13. Installing the program

8. After installation, Setup informs you that the installation is successful, and PC-cillin Internet Security has been started. Click **Finish** to exit Setup.

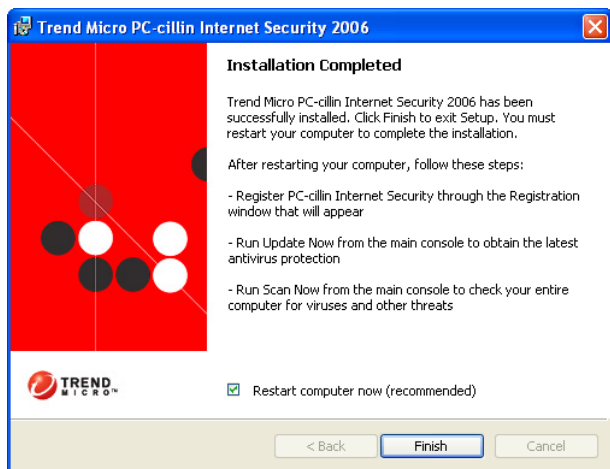


FIGURE 2-14. Installation Completed screen

9. Restart the computer to finish the program registration and startup.

Note: If you choose to restart later, the components may not start properly. Restart your computer as soon as possible.

After installation, refer to [page 37](#) for instructions to help you maximize the program's functionalities.

After Installation

Follow the post-installation steps specified in [Get Started](#) starting on page 37.

Uninstall PC-cillin Internet Security

Before removing PC-cillin Internet Security, close all other open programs. During removal, PC-cillin Internet Security deletes all quarantined files. These files may contain viruses and should not be left on your computer. If you must preserve them, restore the files to a safe, isolated location such as a specially marked floppy disk before removing the program.

Note: Log on to the computer as an Administrator or a user with Administrator privileges. Setup requires a user with Administrator privileges to remove the program components from your computer.

To uninstall PC-cillin Internet Security:

1. Do one of the following:
 - Click **Start > Trend Micro PC-cillin Internet Security 2006 > Uninstall PC-cillin Internet Security**.

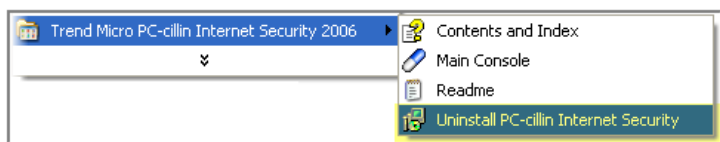


FIGURE 2-15. Uninstalling the product from the Windows Start Menu

- Open Control Panel and then double-click **Add or Remove Programs**. The list of currently installed programs appears. Click **Trend Micro PC-cillin Internet Security 2006**.

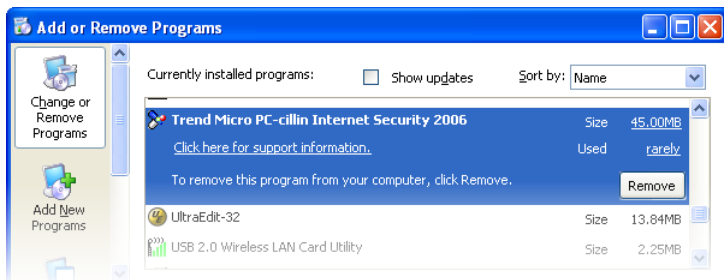


FIGURE 2-16. Uninstalling the product from Control Panel

- Click **Start** > **Run**, type the command shown below, and then click **OK**.

```
msiexec /x {EA8C73AA-3D75-44C9-87A2-8E945FC5FEE6}
```

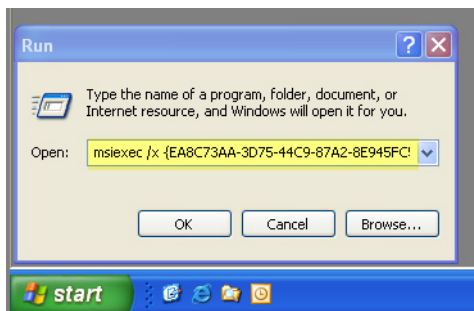


FIGURE 2-17. Uninstalling the product by running the uninstall command

Note: Close all open programs before running the command.

- Use the PC-cillin Internet Security Support Tool, `PCCTool.exe` (see [page 36](#)).

WARNING! Use the Support Tool only if you experienced issues when installing, configuring, or uninstalling the program.

- Click **Yes** to remove the program.
- If password protection is enabled, type the password, and then click **OK**.



FIGURE 2-18. Password prompt before removing the program.

- Restart your computer for the configuration changes to take effect.

Uninstall the Program Using the Support Tool

The Support Tool lets you manually configure specific program modules and functionalities.

To uninstall the program using the Support Tool:

1. Using Windows Explorer, navigate to the directory where the program is installed. For example, C:\Program Files\Trend Micro\Internet Security 2006.
2. Double-click PCCTool.exe. The Support Tool window appears.

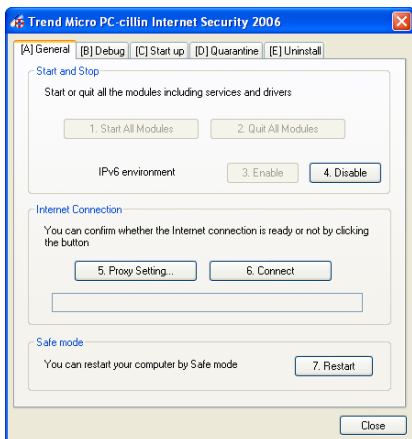


FIGURE 2-19. The Support Tool window

3. Go to the **[E] Uninstall** tab.
4. Click the **4. Uninstall** button.
5. On the prompt that appears, click **Uninstall** to remove the program.

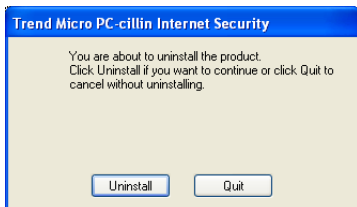


FIGURE 2-20. You cannot cancel after clicking *Uninstall*. This action cannot be undone.

The Support Tool removes the program files, registry entries, and other components. Restart your computer to complete the process.

Trend Micro recommends performing specific tasks after installing and activating PC-cillin Internet Security.

The topics discussed in this chapter include:

- *Register or Activate the Product* on page 38
- *Verify a Successful Installation* on page 42
- *Access the Main Console* on page 43
- *Check Current Settings* on page 45
- *Update Components* on page 46
- *Password-protect the Program* on page 50
- *Obtain More Help* on page 51

Register or Activate the Product

Register or activate your version of PC-cillin Internet Security to enable the product's features.

- **Standard version**—register by following the on-screen instructions that appear after you install the product

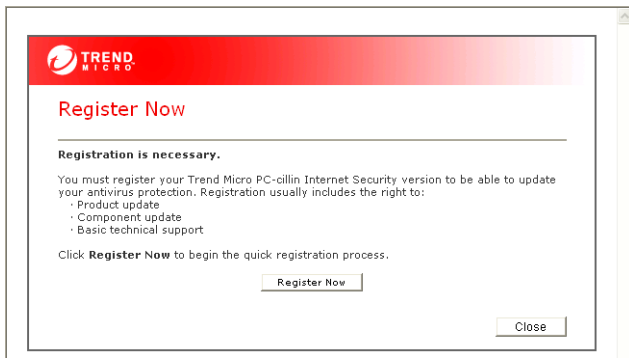


FIGURE 3-1. Use the Register Now page to register a standard version

Depending on the purchase agreement, the standard version is valid for a specific number of months until the limited grace period ends. Renew the product maintenance for continued protection.

- **Evaluation or OEM version**—activate the product by following the onscreen instructions that appear after installation

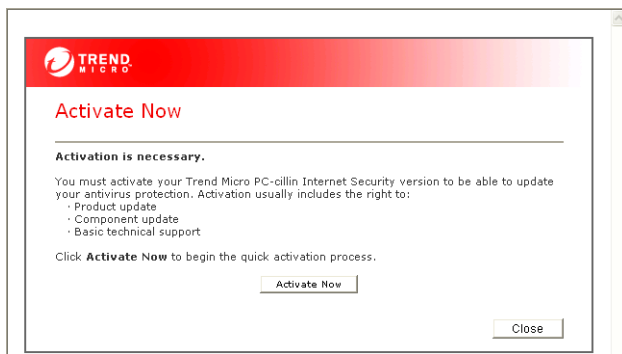


FIGURE 3-2. Use the Activate Now page to register an evaluation or OEM version

The evaluation and OEM versions are fully functional for a limited number of days, after which PC-cillin Internet Security continues to load but scanning, filtering, component updates, and other product features are NOT available. Upgrade to and register the standard version for continued protection.

To register a standard version or activate an evaluation or OEM version:

Do one of the following steps:

- Follow the instructions that appear after installation, refer to [page 39](#)
- Open the Registration / Upgrade / Renewal screen from the main console, refer to [page 40](#)

Use the Registration/Activation Page

The Registration/Activation page appears after successfully installing the program and restarting your computer.

To register a standard version:

1. On the Register Now page (see Figure 3-1), click **Register Now**.
2. A Security Alert message box opens. Click Yes to use a secure connection to the Trend Micro Online Registration server.

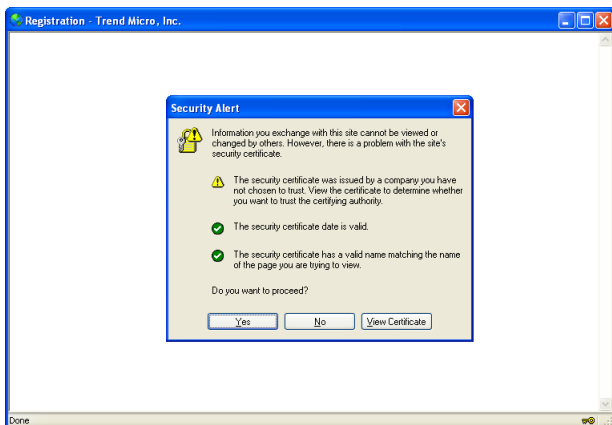


FIGURE 3-3. Security Alert message box

3. If this is your first time to register PC-cillin Internet Security, select **Register without a Customer Care Center account**. Otherwise, if you are upgrading from a previous version, select **Register with a Customer Care Center account**.
4. Follow the on-screen instructions.

To activate an evaluation or OEM version:

1. On the Activate Now page (see Figure 3-2), click **Activate Now**.
2. Provide the required information, and then click **Submit**.

Use the Main Console

Use the Registration / Upgrade / Renewal screen to register/activate the program from the main console.

To register a standard version or activate an evaluation or OEM version:

1. Access the main console (see [page 43](#)).
2. On the PC-cillin Internet Security main console, click **General > Registration / Upgrade / Renewal**.

Tip: Alternatively, click **Register Now** on the Overview screen.

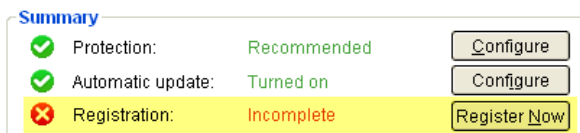


FIGURE 3-4. Registering/Activating the product from the main console > Overview screen

3. A Security Alert message box opens (see Figure 3-3). Click **Yes** to use a secure connection to the Trend Micro Online Registration server.
4. On the Register Now page, click **Register Now**.
5. If this is your first time to register PC-cillin Internet Security, select **Register without a Customer Care Center account**. Otherwise, if you are upgrading from a previous version, select **Register with a Customer Care Center account**.
6. Follow the on-screen instructions.

A page appears informing you of the successful activation/registration and expiration information. The Trend Micro Online Registration server sends a confirmation email message to the address you specified during activation/registration (see Figure 2-1 for a sample).

Depending on the Internet connection and the traffic being processed by the Online Registration server, the Registration status might take a while to refresh. Click **Check Now** on the main console to update the registration status.

When the status refreshes, the main console reflects the current expiration date.



FIGURE 3-5. The status after activating an evaluation or OEM version

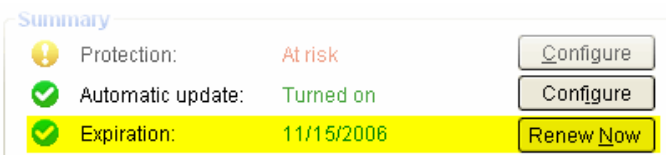


FIGURE 3-6. The status after registering the standard version

After successfully activating/registering the product, you can now download component updates. Refer to [Get Started](#) on page 37 for a complete list of post-installation tasks.

For instructions on how to upgrade to or renew a standard version, please refer to the *Online Help > How To... > Register, Upgrade, or Renew* section.

Verify a Successful Installation

Trend Micro recommends using the European Institute for Computer Antivirus Research (EICAR) test script as a safe way to confirm that PC-cillin Internet Security virus scanning is running and working properly.

Note: The EICAR file is a text file with a *.com extension. It is inert. It is not a virus, it does not replicate, and it does not contain a payload. Never use real viruses to test your antivirus installation.

To verify a successful installation:

1. Open a supported Web browser (see [page 21](#)), and go to <http://www.trendmicro.com/en/security/test/overview.htm>.
2. Download the EICAR test file by clicking one of the eicar.com links. For example, eicar.com (HTTP).

PC-cillin Internet Security detects EICAR as `eicar_virus`, quarantines `eicar_test.com`, displays the Real-time Protection Notification, and logs the event.

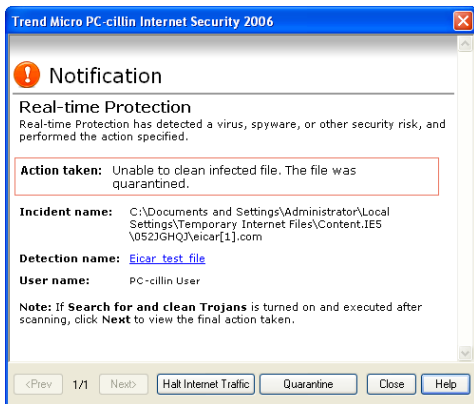


FIGURE 3-7. A sample Real-time Protection Notification

Access the Main Console

The interface of PC-cillin Internet Security provides quick access to all areas of your antivirus, antispyware, antifraud, network security, and general settings.

To access the PC-cillin Internet Security main console:

- Click **Main Console** from the Trend Micro PC-cillin Internet Security 2006 folder on the Windows Start menu
- Double-click the PC-cillin Internet Security icon on the system tray

Note: The system tray is next to the clock, on the bottom-right corner of your screen.

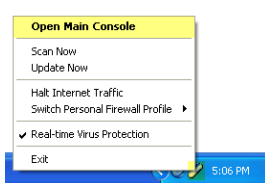


FIGURE 3-8. Accessing the main console from the system tray

- In the system tray, right-click the PC-cillin Internet Security icon and click **Open Main**.

The PC-cillin Internet Security Main window appears.



FIGURE 3-9. The Main Console

Check Current Settings

Access the main console to check your protection settings (see [page 43](#)).

The Overview screen is the landing screen when opening the main console. It provides a summary of the following areas, including links that quickly take you to the appropriate screens where you can configure the settings:

- **Last update**—the date when the program performed the latest manual or automatic update
- **Last scan**—the date when the program finished the latest Complete Scan

After installing the product, **Last update** and **Last scan** are blank because component update and Complete Scan have not run.

Click **Update Now** to manually update the antivirus and content security components.

Tip: If you are part of a network that uses a proxy server to connect to the Internet, configure the proxy server settings to successfully complete an update.

Click **Scan Now** to detect and eliminate viruses, Trojans, worms, spyware, and other grayware present on your computer.

- **Protection**—the status of your computer's protection (Recommended or At risk)

If at least two features are turned off, the level is At risk.

By default, Trend Micro turns on the recommended features. To customize the features according to your environment, click **Configure**.

- **Automatic update**—the status of the automatic/scheduled update (Turned on or Turned off)

By default, PC-cillin Internet Security checks for and downloads updated components every three hours.

- **Registration/Expiration**—if you have not registered a standard version or activated an evaluation/OEM version, the status is **Registration: Incomplete**

Make sure to register PC-cillin Internet Security right after finishing with the installation (see [page 38](#)).

If you have registered/activated the product, the status is **Expiration: <date>**, where **<date>** is the expiration date. The expiration date depends on the license purchased.

Update Components

You must register or activate the product to be able to perform updates.

Note: Within a few moments after installing the product and restarting your computer, PC-cillin Internet Security will check for and automatically download the latest components. After installing the product, but before registering online, you are permitted to update only once. Once you close this window, you must register online to perform the next update.

To update the antivirus and content security components:

- Automatically download the latest components based on a schedule (see [page 46](#))
- Manually update components (see [page 47](#))

Automatically Update Components

Configure PC-cillin Internet Security to regularly check the ActiveUpdate server and automatically download any available components.

Tip: During times of virus outbreaks, Trend Micro can update virus pattern files more than once each week. The scan engine is updated regularly, but less frequently than the pattern file. Trend Micro recommends updating daily (or even more frequently in times of virus outbreaks) to help ensure the program has the current component versions.

To automatically download the latest components based on a schedule:

1. Access the main console (see [page 43](#)).
2. Do one of the following:
 - Click **Overview > Automatic update > Configure**

- Click **General > Update > Automatic Update** tab

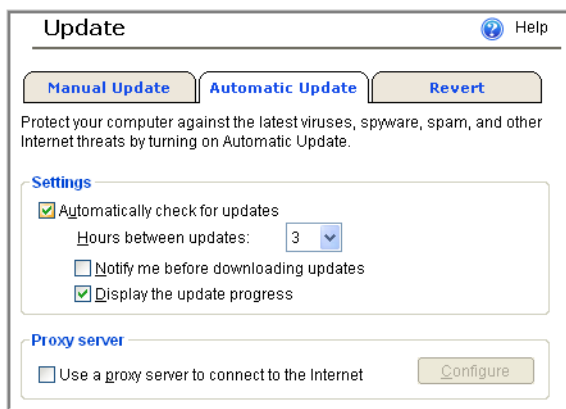


FIGURE 3-10. Setting the automatic update schedule and proxy server settings using the *Automatic Update* tab

3. Select **Automatically check for updates.**

By default, the program enables automatic update every three hours. To check for updates twice a day, set **12** as the **Hours between updates**.

Note: If you are part of a network that uses a proxy server to connect to the Internet, be sure to configure the proxy server settings.

4. To receive a notification and view the progress while updating, select **Notify me before downloading updates and **Display the update progress**.**

Manually Update Components

Manually update the antivirus and content security components immediately after installing PC-cillin Internet Security. This establishes a baseline of security for your computer.

Tip: Trend Micro suggests you perform a manual update whenever a threat outbreak is occurring, or if you suspect that your computer is infected, but a scan did not detect any threats.

To manually update components:

1. Access the main console (see [page 43](#)).
2. Do one of the following:
 - Click **Overview**
 - Click **General > Update > Manual Update** tab

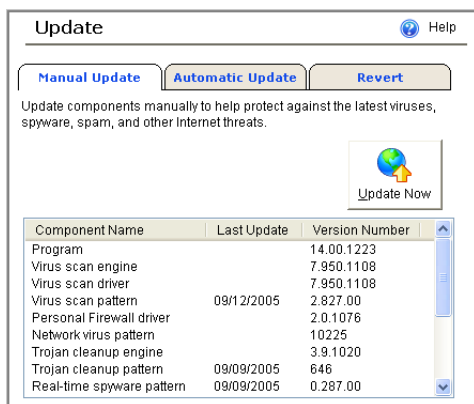


FIGURE 3-11. The Manual Update tab

3. Click **Update Now**.

Note: If you are part of a network that uses a proxy server to connect to the Internet, be sure to configure the proxy server settings.

PC-cillin Internet Security checks for and downloads the latest components. If the components being used are current, the following message appears:

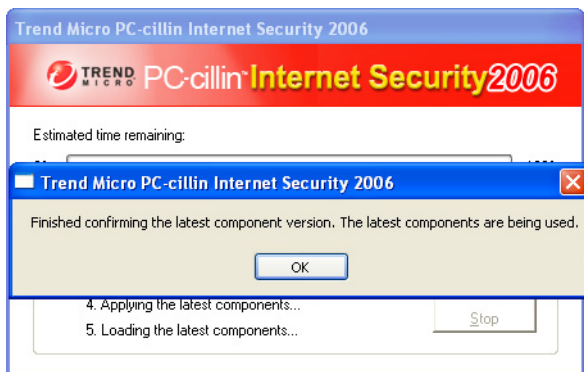


FIGURE 3-12. Components are up to date

Query Update Logs to check the results of the update process. Refer to the *Online Help > Contents & Index > Monitor Events* section for instructions about how to query logs.

Password-protect the Program

Set a password to protect your computer by preventing other people from disabling or changing your settings. Using the Private Network Protection or Wi-Fi Intrusion Detection requires you to set a password.

The password protects the following features:

- All Antivirus menu options
- All Antispyware menu options
- Antifraud Wizard
- Private Network Protection
- Web Site Filter
- General > Preferences
- Privacy Protection
- Spam and Fraud Filters
- Scan settings
- Mail Scan
- Webmail Scan
- Program exiting
- Uninstallation



FIGURE 3-13. If password protection is set, unauthorized actions such as uninstalling the program are prevented

To set your password:

1. On the main console, click **General > Preferences**.
2. Under **Password**, select **Password-protect settings**. A window appears that will allow you to set the password.
3. Provide the password in the **Type password** and **Confirm password** fields.

Tip: The password must contain at least six characters, and can include only letters of the alphabet (upper or lower case) and numbers (0 through 9). Refer to the *Online Help > Tips > Establishing Strong Passwords* topic for recommended password practices.

4. Click **OK** to save.
5. On the Preference screen, click **Apply**. The features listed at the beginning of this section are now password protected.

Obtain More Help

PC-cillin Internet Security offers various types of online help.

To get help while using the program, do one of the following:


HELP OPTION	DESCRIPTION
Contents and Index	Select Contents and Index from the header menu to learn about the program features and configuration recommendations.
 Help (Context-sensitive help icon)	Click the help icon to learn about a particular main console page.
Mouseover help	Hover the mouse on the icon to read a description of the options.
Knowledge Base	Select Knowledge Base from the header menu or help pages to access troubleshooting and FAQ information.
Security Info	Select Security Info from the header menu to open the Trend Micro Virus Security Web site and access general information about computer security threats, and virus alerts.

TABLE 3-1. Online help options

Problem Solving and FAQ

This chapter explains how to solve problems that you may encounter while using PC-cillin Internet Security.

The topics discussed in this chapter include:

- *Installation* on page 54
- *Registration/Activation* on page 56
- *Main Console Access Issues* on page 57
- *Component Update Issues* on page 58
- *Frequently Asked Questions* on page 59

Installation

One of the following issues may occur during PC-cillin Internet Security installation:

- Setup stops responding
- Setup reports a successful installation, but PC-cillin Internet Security services are not started
- Setup stops because the minimum system requirements are not met

To troubleshoot installation issues:

1. Make sure that you have logged into your computer where you want to install PC-cillin Internet Security with Administrator privileges.



FIGURE 4-1. In Windows 2000, press **Ctrl + Alt + Del** simultaneously to confirm that you are using an account with Administrator privileges

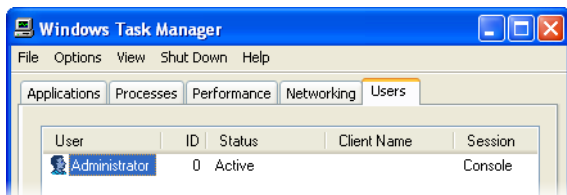


FIGURE 4-2. In Windows XP, go to the **Users** tab to check the account

2. Review the section *Install PC-cillin Internet Security 2006* and confirm that all instructions were followed.

3. Verify that your computer meets the minimum requirements (see [page 26](#)).
4. If you still cannot install the product, contact your Trend Micro support provider (see [page 66](#)).

Registration/Activation

One of the following issues may occur during registration or activation:

- Invalid or missing serial number
- Unable to register/activate the product after installation or through the main console

To troubleshoot product registration issues:

1. Verify that you have entered the serial number correctly. You must provide this information in the following format:

XXXX-XXXX-XXXX-XXXX-XXXX

Note: Each X corresponds to a number or letter. You can type the letters in either uppercase or lower case.

2. See if you can find any relevant warning messages or log information related to registration or activation. You can search for solutions based on this information.

Tip: Refer to the *Online Help > Monitor Events* section for instructions about how to query logs.

3. Make sure that you have used a valid license.

You can only use the software for free during a limited grace period. Make sure to upgrade or renew your license before the grace period expires to help keep your computer safe. If necessary, contact your reseller to obtain upgrades or purchase a new serial number.

4. If the above steps do not work, contact your Trend Micro support provider (see [page 66](#)).

Main Console Access Issues

You may encounter one of the following problems when trying to open the main console of PC-cillin Internet Security:

- You cannot open the main console
- The main console does not recognize your password

To help solve these main console access issues:

1. Make sure that you installed the program successfully (see [page 42](#)).
2. Use the Windows **Services** panel to make sure that the **Trend Micro Real-time Service** has started.

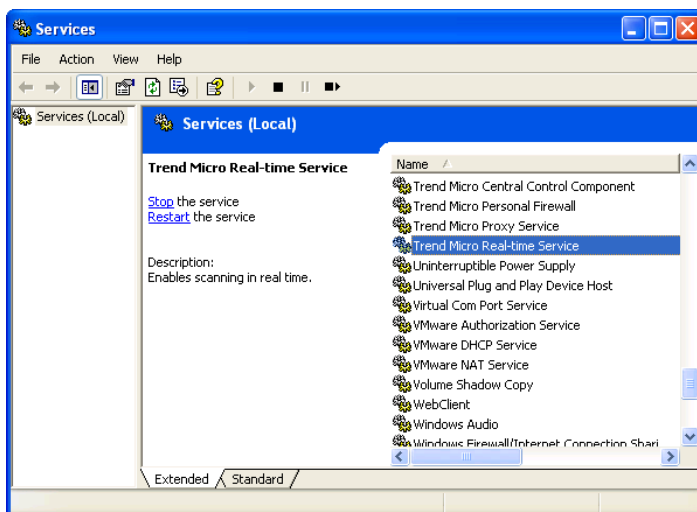


FIGURE 4-3. Make sure that the Trend Micro Real-time Service has started

3. If the above steps do not work, contact your Trend Micro support provider (see [page 66](#)).

Component Update Issues

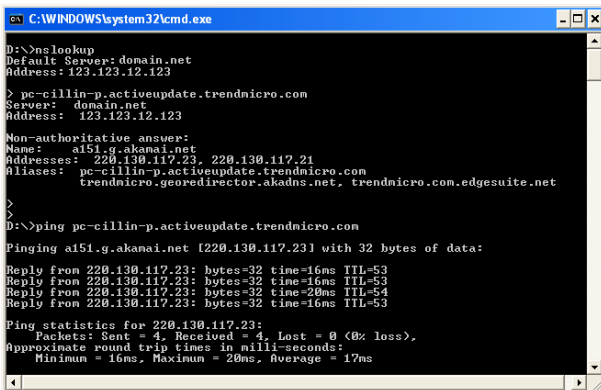
If you configured PC-cillin Internet Security to download antivirus and content security components from **Trend Micro ActiveUpdate** but cannot download the latest components, check your connection to the ActiveUpdate server.

To help solve an ActiveUpdate issues:

1. Make sure your computer has a working connection with the Internet. Also check your network and computer for any obvious hardware or software problems.
2. Open the Windows command prompt by clicking **Start > Run > Open** and typing `cmd` in the window that opens.
3. Issue the following commands to make sure your computer can resolve the ActiveUpdate server's Fully Qualified Domain Name (FQDN).

```
nslookup
```

```
ping
```



```
C:\WINDOWS\system32\cmd.exe
D:\>nslookup
Default Server: domain.net
Address: 123.123.12.123

> pc-cillin-p.activeupdate.trendmicro.com
Server: domain.net
Address: 123.123.12.123

Non-authoritative answer:
Name: ai51.g.akamai.net
Addresses: 220.130.117.23, 220.130.117.21
Aliases: pc-cillin-p.activeupdate.trendmicro.com
         trendmicro.georedirector.akadns.net, trendmicro.com.edgesuite.net
>

D:\>ping pc-cillin-p.activeupdate.trendmicro.com

Pinging ai51.g.akamai.net [220.130.117.23] with 32 bytes of data:
Reply from 220.130.117.23: bytes=32 time=16ms TTL=53
Reply from 220.130.117.23: bytes=32 time=16ms TTL=53
Reply from 220.130.117.23: bytes=32 time=20ms TTL=54
Reply from 220.130.117.23: bytes=32 time=16ms TTL=53

Ping statistics for 220.130.117.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 20ms, Average = 17ms
```

FIGURE 4-4. Using the command prompt *ping* and *nslookup* commands

4. If the above steps do not work, contact your Trend Micro support provider (see [page 66](#)).

Frequently Asked Questions

This section provides answers to questions related to the following subjects:

- *General* concepts
- *Serial Number, Installation, and Registration*

General

- What is PC-cillin Internet Security?
- How does PC-cillin Internet Security protect my computer?
- Can PC-cillin Internet Security filter offensive content found in email messages, attachments, and instant messages?
- Can PC-cillin Internet Security filter content of all file types?
- What are the instant messaging clients that PC-cillin Internet Security supports?
- What Internet browsers can I use with PC-cillin Internet Security?
- What is phishing?

Serial Number, Installation, and Registration

- Why is my registration still *Incomplete* even though I have successfully registered/activated the product?
- What if I lose my serial number?

Note: Please refer to the PC-cillin Internet Security *Online Help > Contents & Index > Frequently Asked Questions* section for answers to configuration related questions.

What is PC-cillin Internet Security?

PC-cillin Internet Security protects your computer from both external and internal threats. Please refer to [Table 1-1](#) for details about the product's protection features.

How does PC-cillin Internet Security protect my computer?

PC-cillin Internet Security provides the following types of protection:

- Antivirus—Real-time Virus Protection, Scheduled and Manual Scan
- Antispyware—Real-time Spyware Protection, Scheduled and Manual Scan

Refer to the PC-cillin Internet Security *Online Help > Contents & Index > Learn About...* section for details about these features.

Can PC-cillin Internet Security filter offensive content found in email messages, attachments, and instant messages?

No. The product does not filter content found in these media. However, PC-cillin Internet Security can check for and help eliminate viruses, Trojans, worms, spyware, spam, and other threats in email messages and attachments.

Can PC-cillin Internet Security scan for viruses and other types of malware in all file types?

Yes. The Antivirus feature provides the options to set the type of files that the product will scan.

What are the instant messaging clients that PC-cillin Internet Security supports?

Privacy Protection can prevent private information from being sent using one of the following instant messaging clients:

- AOL Instant Messenger 5.9
- ICQ 5 or ICQ Lite
- MSN Messenger 7.0
- Windows Messenger 4.7 or 5.1

What Internet browsers can I use with PC-cillin Internet Security?

Privacy Protection and Web Site Filter support the following browsers:

- AOL Browser 9.0
- Internet Explorer 5.5 or 6.0
- Mozilla Firefox 1.0
- Netscape Navigator 7.2

What is phishing?

Phishing is a rapidly growing form of fraud that seeks to fool Web users into divulging private information by mimicking a legitimate Web site.

Phishers use the following forms of attacks:

- Email messages

An unsuspecting user gets an urgent sounding, authentic looking email message telling him or her there is a problem with their account. They must immediately fix the problem, or the account will be closed. The message will include a link that redirects users to a fake Web site.

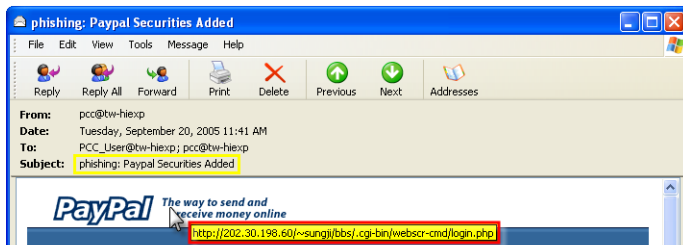


FIGURE 4-5. A sample phishing email message

- Web sites

A fraudulent Web site looks similar to the actual page. Any data entered at the site is directed to a malicious hacker who steals the logon name,

password, credit card number, social security number, or whatever data s/he requests.



FIGURE 4-6. A sample phishing Web site

- Internet Relay Chat (IRC) and instant messaging (IM) programs
Since many IRC and IM programs allow you to send embedded dynamic content (for example, graphics, Web site addresses, multimedia), phishers can actually employ techniques used in standard Web-based attacks through messaging clients.

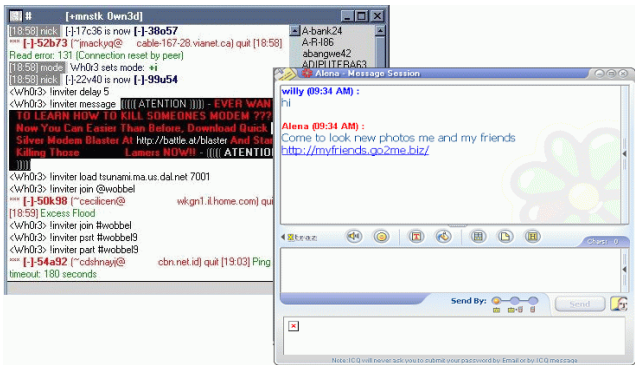


FIGURE 4-7. Sample phishing instant messages

Why is my registration still *Incomplete* though if I have successfully registered/activated the product?

In some cases, depending on your network connection, the response from the Online Registration server might be delayed. While waiting, check whether you can run Update Now. If so, product registration was successful. The status will change to Registered.

What if I lose my serial number?

Please contact your regional Trend Micro technical support representative.

- Email—support@support.trendmicro.com
- Web site—
<http://kb.trendmicro.com/solutions/Srf/questionEntry.asp>

Trend Micro is committed to providing service and support that exceeds user's expectations. This chapter contains information on how to get technical support. Remember, you must register your product to be eligible for support.

This chapter includes the following topics:

- *Contact Technical Support* on page 66
- *Send Infected File Samples* on page 67
- *Report Spam, Fraudulent, and Incorrectly Tagged Messages* on page 67
- *TrendLabs* on page 67
- *Other Useful Resources* on page 68

Contact Technical Support

Before contacting technical support, here are two things you can quickly do to try and find a solution to your questions:

- **Check your documentation:** the *Problem Solving and FAQ* chapter of this *Getting Started Guide* and *Online Help* provide comprehensive information about PC-cillin Internet Security
Search both documents to see if they contain your solution.
- **Visit our Technical Support Web site:** our Technical Support Web site contains the latest information about all Trend Micro products
The support Web site has answers to previous user inquiries. To search the Knowledge Base, visit

<http://kb.trendmicro.com>

In addition to phone support, Trend Micro provides the following resources:

- Email support
- Readme: late-breaking product news, installation instructions, known issues, and version specific information
- Product updates and patches

<http://www.trendmicro.com/download/>

To locate the Trend Micro office nearest you, open a Web browser to the following URL:

<http://www.trendmicro.com/en/about/contact/overview.htm>

To speed up the issue resolution, when you contact our staff please provide as much of the following information as you can:

- PC-cillin Internet Security serial number
- Version
- Exact text of the error message, if any
- Steps to reproduce the problem

Send Infected File Samples

You can send viruses, infected files, Trojan programs, spyware, and other grayware to Trend Micro. More specifically, if you have a file that you think is some kind of threat but the scan engine is not detecting it or cleaning it, you can submit the suspicious file to Trend Micro using the following Web address:

<http://subwiz.trendmicro.com>

Please include in the message text a brief description of the symptoms you are experiencing. Our team of virus engineers will "dissect" the file to identify and characterize any viruses it may contain.

Report Spam, Fraudulent, and Incorrectly Tagged Messages

Report spam messages to false@support.trendmicro.com. Report fraudulent messages to antifraud@support.trendmicro.com. Report incorrectly tagged messages or false positive detections to false@support.trendmicro.com.

Trend Micro Technical Support replies to your message within twenty four hours.

TrendLabs

Trend Micro TrendLabsSM is a global network of antivirus research and product support centers that provide continuous 24 x 7 coverage to Trend Micro customers around the world.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers in Paris, Munich, Manila, Taipei, Tokyo, and Irvine, CA. ensure a rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

For more information about TrendLabs, please visit:

<http://www.trendmicro.com/en/security/trendlabs/overview.htm>

Other Useful Resources

Trend Micro offers a host of services through its Web site, www.trendmicro.com.

Internet-based tools and services include:

- Virus Map—monitors virus incidents around the world
- HouseCall™—Trend Micro online virus scanner
- Virus risk assessment—the Trend Micro online virus protection assessment program for corporate networks

Index

A

- access main console 43
- Acrobat 21
- activation 38
 - evaluation version 38
 - using the Activate Now page 39
 - using the main console 40
- activation issues 56
- ActiveUpdate 58
- Administrator 22
- Administrator account 34
- Antifraud Toolbar 10
- Antifraud Wizard 10
- Antiphishing 8
- Automatic update 45
- Automatic Update tab 47

B

- Back 18
- before contacting support 66
- beta version 23

C

- CD 27
- common program buttons 18
- Complete Scan 9
- Configure 18
- confirm Virus Scan 42
- CPU 20
- current settings 45
- Customer Care Center 40

D

- document conventions 3
- documentation 2
- documentation audience 3

E

- EICAR, eicar.com. See test virus
- email software 20

- evaluation 23
- evaluation version 38
- Expiration 45
- extra Hosts file entry blocking 11, 15

F

- FAQs. See frequently asked questions
- footer menu 18
- FQDN 58
- Fraud Filter 8
- Fraud Filters 15
- fraudulent email messages 61
- fraudulent messages 8
- fraudulent Web sites 9, 61
- frequently asked questions
- Full installation 7, 31

G

- Getting Started Guide 2
 - about 2
- Getting Started Tutorial 2
- GSG. See Getting Started Guide

H

- Halt Internet Traffic 18
- hard disk space 20
- hardware and software requirements 22
- hardware requirements 20
- header menu 17
- help 2, 51
- Hosts file 11
- HouseCall 68

I

- Incomplete registration/activation 59
- installation
 - Full 31
 - issues 54
 - Minimum 31
 - minimum 7

- preparation 22
- steps 26
- type 31

Installation Completed screen 33

Installation Folder screen 30

Installation Type screen 31

instant messages

instant messaging clients 21

Internet connection 21

Internet Relay Chat 62

invalid serial number 56

IRC. See Internet Relay Chat

L

Last scan 45

Last update 45

launching Setup 26

license agreement screen 28

M

Mail Scan 15

mail services 20

Mail User Agent 20

main console, footer menu, header menu, main menu, working menu 17

main menu 17

Manual Update tab 48

manual Vulnerability Check 12

memory 20

Minimal installation 7

- excluded features 7

Minimum installation 31

missing serial number 56

msiexec 35

MUA

- See Mail User Agent

N

new features 6

nslookup 58

O

obtain help 51

OEM 23, 38

OEM version 38

online help 2

Online Registration server 39

operating system 20

original equipment manufacturer 23

Overview screen 40, 41

P

page

- Activate Now 38

- Register Now 38

password protection 50

pattern file rollback. See Revert 13

PCCTool.exe 35

Personal Firewall 15

pharming 10

phish/phishing

- See Antiphishing

phishing

- fraudulent email messages 61

- fraudulent instant messages

- fraudulent Web sites 61

ping 58

Popup Manager 13

popup messages 13

pre-installation tasks 22

printed documentation 2

Privacy Protection 15

problem solving

- activation 56

- component update 58

- installation 54

- registration 56

- update 58

protection

- default 16

- features 15

- status 45

protection features 15

R

Ready to Install screen 32

Real-time Network Virus Protection 15

- Real-time Protection Notification 42
- Real-time Scan icon 18
- Registration 45
- registration 38
 - standard version 38
 - using the main console 40
 - using the Register Now page 39
- registration issues 56
- removing
 - See uninstall
- reporting false positives 67
- resolution 21
- restart 33
- Revert 13
- rollback. See Revert 13

S

- Scan Now 18
- scheduled Vulnerability Check 12
- screen
 - Antifraud Wizard 10
 - Antispyware 11
 - Complete Scan 9
 - Installation Completed 33
 - Installation Folder 30
 - Installation Type 7, 31
 - license agreement 28
 - Overview > Registration 40, 41
 - Product Registration 29
 - Ready to Install 32
 - Revert 13
 - scanning Trojans 29
 - Vulnerability Check 12
 - Web Site Filter 9
 - Welcome 28
- sending infected file samples 67
- serial number
 - invalid or missing 56
 - providing 30
- Services 57
- services 57
- setup.exe 27
- software requirements 20
- Spam Filter 15

- spoofed domain name blocking 11
- Spyware Scan 15
- standard 38
- support 65, 66
 - contacting support 66
 - email 66
 - Knowledge Base 66
 - speeding up resolution 66
- Support Tool 35
- system Hosts file. See Hosts file
- system tray 43
- system tray icons 18

T

- test virus 42
- third-party antivirus 22
- tips
 - documentation 2
 - querying logs 56
- Trend Micro Real-time Service 57
- TrendLabs 67
- troubleshooting
 - component update 58

U

- uninstall
- update 46
 - automatic 46
 - manual 47
- Update Center 2
- update issues 58
- Update Now 18
- Updating components 18
- upgrade 23

V

- verify installation 42
- Virus Map 68
- virus risk assessment 68
- Virus Scan 15
- Vulnerability Check 15
 - manual 12
 - scheduled 12

W

Web server 22

Web Site Filter 9

- extra Hosts file entry blocking 11

- spoofed domain name blocking 11

Welcome screen 28

what's new 6

Wi-Fi Intrusion Detection 15

Windows Start menu 34

working area 17